

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-232960

(43)Date of publication of application : 14.09.1990

(51)Int.Cl.

H01L 27/04
H01L 21/82
H01L 29/788
H01L 29/792

(21)Application number : 02-004397

(71)Applicant : GENERAL INSTR CORP

(22)Date of filing : 11.01.1990

(72)Inventor : GILBERG ROBERT C
KNOWLES RICHARD M
MORONEY PAUL
SHUMATE WILLIAM A

(30)Priority

Priority number : 89 297472 Priority date : 12.01.1989 Priority country : US

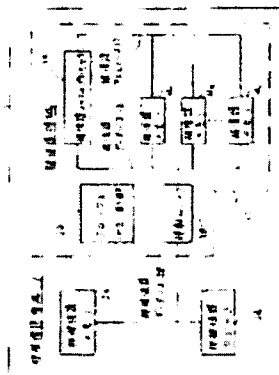
(54) INTEGRATED CIRCUIT CHIP

(57)Abstract:

PURPOSE: To ensure an integrated circuit chip of data protection by a method wherein a semiconductor layer is partitioned into a protected region and a non-protected region, a microprocessor and a memory to protect are provided in the protected region, and a memory and a logic which control them are provided in the non-protected region, and the two partitioned regions are connected with a conductive layer.

CONSTITUTION: An IC chip 10 is partitioned into a protected region 11 and a non-protected region 12, wherein a microprocessor 14 which processes the protected data, memories M1 to M4 which store the protected data, a data bus 16, an address bus 17, a transfer logic circuit 18, and a circuit 20 which

controls clock and a power are provided in the protected region 11. A non-protected memory 24 and a non-protected logic 26 are provided in the non-protected region 12, and the outputs of them are inputted into the logic 18 located in the region 11 through the intermediary of the data bus 28. Thereafter, signals selected by the logic 18 are inputted



into the prescribed device located in the region 11, whereby the protected data are prevented from being erroneously inspected and modified.

⑫ 公開特許公報(A) 平2-232960

⑬ Int.Cl.⁵

識別記号

庁内整理番号

⑭ 公開 平成2年(1990)9月14日

H 01 L 27/04

A

7514-5F

7514-5F

8526-5F

H 01 L 29/78

21/82

3 7 1

D※

審査請求 未請求 請求項の数 24 (全13頁)

⑮ 発明の名称 集積回路チップ

⑯ 特 願 平2-4397

⑰ 出 願 平2(1990)1月11日

優先権主張 ⑱ 1989年1月12日 ⑲ 米国(U S) ⑳ 297,472

⑳ 発 明 者 ロバート・シー・ギル アメリカ合衆国、カリフォルニア州 92131、サンディエ
バーグ カミニート・ガルシア 11484㉑ 発 明 者 リチャード・エム・ノ アメリカ合衆国、カリフォルニア州 92126、サンディエ
ウルズ ゴ、ヘンブヒルウェイ 10323㉒ 出 願 人 ジエネラル・インスト アメリカ合衆国、ニューヨーク州、10153 ニューヨー
ルメント・コーポレー ク、フィフス・アベニュー 767
ション

㉓ 代 理 人 弁理士 鈴江 武彦 外3名

最終頁に続く

明 細 書

1. 発明の名称

集 積 回 路 チ ャ ッ プ

2. 特許請求の範囲

(1) 被保護データが処理並びに／又はストアされる被保護領域(11)を有する集積回路チップ(10)であり、

回路要素部品を形成する拡散部分(S, D)を有する半導体層(SC)と、

被保護データを配分、ストア、処理並びに／又は変更をするための回路要素(14, 16, 17, 18, 20, M₁, M₂, M_N)を形成する要素相互を接続するように前記半導体層と結合される第一導電層(CN₁)と、

前記回路要素が検査からシールドされた被保護領域(11)を形成するように回路要素を覆うと共に、回路要素の予期機能に対し、必須の所定の信号を回路要素に送り込むために回路要素と接続された第2導電層(CN₂)とを具備し、前記第2導電層の除去は、所定の必須の信号が回路要素へ送ら

れることを妨げ、予期機能をはばむ集積回路チップ。

(2) 前記所定の信号がパワー信号である請求項(1)に記載の集積回路チップ。

(3) 前記シールドされた回路要素が被保護データをストアするための揮発性メモリ(M₁, M₂, M_N)を有し、このメモリは所定のパワー信号で動かされる請求項(2)に記載の集積回路チップ。

(4) 前記揮発性メモリ(M₁, M₂, M_N)が夫々個別に、夫々のメモリと第2導電層(CN₂)の重った場所のみから所定のパワー信号を受けられるように第2導電層のその場所のみと接続されたメモリである請求項(3)に記載の集積回路チップ。

(5) 非被保護データと制御信号が処理並びに／又はストアされ、前記のシールドされた回路要素は被保護領域(11)と非被保護領域(12)間の非被保護データ並びに／又は制御信号のトランスファーを可能にする所定のパワー信号で動作するロジック回路要素(18)を含むような非被保護領域(12)を

さらに具備した請求項(2)に記載した集積回路チップ。

(6)前記のロジック回路要素(18)が夫々個別に第2導電層の重なった場所からのみ所定のパワー信号を受けるようにロジック回路要素と重なった第2導電層(CN₂)のその場所に別々に接続されている請求項(5)に記載した集積回路チップ。

(7)前記のシールドされた回路要素(14,16,17,18,20,M₁,M₂,M_N)が夫々個別に第2導電層の重なった場所のみからのみ所定のパワー信号を受けるようにシールドされた回路要素と重なった第2導電層(CN₂)のその場所に別々に接続されている請求項(2)に記載した集積回路チップ。

(8)前記の第1導電層のシールドされた回路要素は被保護データをストアするためのメモリ(M₁,M₂,M_N)と、そのメモリにストアされる駆動データ用のロジック回路(14)を有し、その第2導電層(CN₂)はロジック回路の駆動機能にとって必須である信号を導き、そしてこの第2導電層の除去はこのメモリにデータがストアさ

メモリロケーションにストアさせるのを妨げるためにフューズ要素とメモリ制御回路とアドレスバスとに接続されたデテクター(40)と

を備えた請求項(1)に記載された集積回路チップ。

(10)前記第2導電層(CN₂)が更にメモリ(M)と、メモリ制御ロジック回路(38)と、デテクター(40)と、フューズ要素(42)とを直接的外部からのアクセスからシールドしている請求項(9)に記載された集積回路チップ。

(11)前記所定の信号が、メモリ(M)と、メモリ制御ロジック回路(38)と、デテクター(40)とが所定のパワー信号で動作されるようなパワー信号である請求項(9)に記載された集積回路チップ。

(12)前記所定の信号がパワー信号であり、メモリ(M)は所定のパワー信号で動作する揮発性メモリである請求項(9)に記載された集積回路チップ。

(13)前記シールドされた回路要素が、
変更不能な被保護データをストアするための所

れることを妨げるような請求項(1)に記載の集積回路チップ。

(9)前記のシールドされた回路要素が変更不能な被保護データをストアするための所定の夫々場所としてメモリロケーションをもったメモリ(M)と、

アドレスバスに伝えられたアドレス信号により指示されたメモリの場所にデータがストアされるためにこのメモリとアドレスバス(46)に接続されたメモリ制御ロジック回路(38)と、

最初の状態と非可逆的に変化した状態を持つフューズ要素(42)と、

所定の制御信号(48)に呼応してフューズ要素の状態を非可逆的に変化させるためのフューズ要素に接続されたもの(44)と、

フューズ要素の状態と所謂アドレス信号をモニターするためと、何時でも所定のメモリロケーションがアドレスバス上でアドレス信号により示されるが、ヒューズ要素が非可逆的に変化してしまったあとではメモリ制御回路がデータを所定のメ

定のメモリロケーションを持っている第1メモリ(M)と、

第2メモリ(52)と、

第2メモリにデータパターンをストアさせる手段(55)と、

第2メモリが所定のデータパターンを持っている時は何時でも書き込み信号(64)に呼応して第1メモリの所定のロケーションにデータをストアさせられるように第1と第2メモリに接続されたメモリ制御ロジック回路(55)と、

第2メモリの内容を消去出来るように第2メモリに接続された手段(68)と、

最初の状態と非可逆的に変化した状態をもつヒューズ要素(50)と、

所定の制御信号(67)に呼応してフューズ要素を非可逆的に変化させるフューズ要素に接続されている手段(58)と、

フューズ要素の状態が非可逆的に変化する前にもみ所謂データパターンがストア出来るようにするデータパターンを第2メモリにストアするもの

に接続されたフェーズ要素とを備えた請求項(1)に記載された集積回路チップ。

(14)前記第2導電層(CN₂)が更にメモリ(M₅₂)と、メモリ制御ロジック回路(54)と、ストレッチ用部品とフェーズ要素とを直接的外部からのアクセスからシールドしている請求項(13)に記載の集積回路チップ。

(15)前述の所定の信号がパワー信号であり、メモリ(M₅₂)とメモリ制御ロジック回路(54)と、ストレッチをさせる部品とが所定のパワー信号で動く請求項(13)に記載の集積回路チップ。

(16)前述の所定の信号がパワー信号であり、第1メモリ(M)が所定のパワー信号で動作する揮発性メモリである請求項(13)に記載の集積回路チップ。

(17)シールドされた回路要素が、
被保護データをストア出来る動作部品(80)と、
最初の状態と非可逆的に変化した状態をもつフェーズ要素(58)と、
所定の制御信号に呼応してフェーズ要素の状態

を非可逆的に変化させる、フェーズ要素に接続された手段(58)とを備え、

そのフェーズ要素がその状態が非可逆的变化をする前にのみ所謂被保護データをストア出来るようにする手段と接続されているような請求項(1)に記載の集積回路チップ。

(18)前記の所定の信号が、パワー信号であり、動作部品(80)は所定のパワー信号で動作する請求項(17)に記載の集積回路チップ。

(19)所謂テスト回路要素に対するアクセス回路要素に対する部品(78)と、

最初の状態と非可逆的に変化した状態をもつフェーズ要素(70)と、

所定の制御信号(80)に呼応してフェーズ要素の状態を変化させる、フェーズ要素に接続された部品(74)とを備え、

そのフェーズ要素が、その状態が非可逆的に変化する前にのみ所謂テストのためにアクセス出来る手段に接続されているような請求項(1)に記載の集積回路チップ。

(20)前記所定の信号はパワー信号であり、作動部品(72,74)は第2導電層により外部よりのアクセスからシールドされ、所定のパワー信号で動作する請求項(19)に記載の集積回路チップ。

(21)前記のシールドされた回路要素に、
被保護データをストアし、処理し、処理に影響を与える前述の回路要素(M)と、

最初の状態と非可逆的に変化した状態をもつフェーズ要素(42)と、

所定の制御信号(48)に呼応してフェーズ要素の状態を非可逆的に変化させる、フェーズ要素に接続された部品(44)と、

フェーズ要素(42)と前記回路要素(M)に接続され、

フェーズ要素の状態をモニターするためと、フェーズ要素の状態が非可逆的に変化してしまったあとで回路要素の予期状態を妨げるための手段(40)が含まれる請求項(1)に記載された集積回路チップ。

(22)シールドされた回路要素には、

被保護データをストアし、処理し、処理に影響を与える前述の回路要素(M)と、

最初の状態と非可逆的に変化した状態をもつフェーズ要素(42,58)と、

フェーズ要素に接続され、所定の制御信号(48,87)に呼応してフェーズ要素の状態を変化させる部品(44,58)を有し、

このフェーズ要素は、その状態が非可逆的に変化する前にのみその回路要素の予期機能が可能となるように回路要素と接続されている請求項(1)に記載した集積回路チップ。

(23)シールドされた回路要素に更に被保護データをストア並びに/又は処理するシールドされた回路要素(14,M₁, M₂, M₃)への供給パワーを制御する手段(20)を有する請求項(1)に記載の集積回路チップ。

(24)シールドされた回路要素に更にクロック信号を発生させそのクロック信号を被保護データをストア並びに/又は処理するシールドされた回路要素(14,M₁, M₂, M₃)に供給する手段(20)

を有する請求項(1)もしくは(23)に記載された集積回路チップ。

3. 発明の詳細な説明

〔従来の技術〕

本発明は一般に電子的データ処理システム用集積回路チップに関し、特に集積回路チップの被保護領域でストアされたり処理された被保護データの検査や修正を防止することを指図する。

被保護データを処理しストアする集積回路チップは被保護データを処理しストアする回路要素をもった被保護領域と、非保護データと制御信号を処理しストアする回路要素をもつ非被保護領域とを備えている集積回路チップは回路要素を形成する拡散部を有する半導体層と、回路要素を形成する部品を内部接続するために前記半導体層と接続された第1導電層を具備する。すべての新しい集積回路チップは代表的には回路要素と部品を相互接続するために1つ或はそれ以上の導電層を有する。一般的にこれ等の層は制御信号とパワー信号両者を伝えるのに使われ、信号の相互接続の密度

を最大とし、そのような相互接続に要な面積を減少させることを目標としている。

この被保護領域は更に、被保護領域内にあるデータ処理回路要素により被保護データを処理するために被保護領域内のデータバスへ非被保護データと制御信号を転送する回路要素を有する、被保護領域内の回路要素は非被保護データと制御信号を非被保護領域と被保護領域内のデータバス間に被保護領域内のデータ処理回路要素により発生された制御信号に応じて転送することができる。

〔発明が解決しようとする課題〕

それにも拘わらず、被保護データでさえこのような集積回路チップでは被保護領域から非被保護領域への転送は容易には出来ず、被保護領域内にストアされたか、処理中の被保護データに例えば走査形電子顕微鏡(SEM)やここから被保護データがアクセス出来る被保護領域内で与えられたノードで顕微鏡に接続されたプローブのような診断装置を使った検査によりアクセスをすることができる。又特定の制御信号を被保護領域内のロジック

回路要素に送ることによりプローブのような方法でロジック回路が被保護データを被保護領域内の非被保護と被保護再データを被保護領域内のデータ処理回路要素により処理するため、データバスから非被保護領域へ転送することが出来るかもしれない。或は被保護領域内のストアされた被保護データはチップの保護を疑わしくされることを意味することが出来内密のデータによりおきかえられるかもしれない。

〔課題を解決するための手段〕

この発明は、回路要素部品を形成する拡散部分を有する半導体層と、

被保護データを配分、ストア、処理並びに／又は変更をするための回路要素を形成する要素相互を接続するように前記半導体層と結合される第一導電層と、前記中で、回路要素が検査からシールドされた被保護領域を形成するように回路要素を覆うと共に、回路要素の予期機能に対し、必須の所定の信号を回路要素に送り込むために回路要素と接続された第2導電層とを具備し、前記第2導

電層の除去は、所定の必須の信号が回路要素へ送られることを防ぎ、予期機能をはばむ、被保護データが処理並びに／又はストアされる被保護領域を有する集積回路チップを提供する。

この発明の一態様においては、前記所定の信号がパワー信号である。この一態様に係わる実施例においては、前記第1の導電層のシールドされた回路要素が被保護データをストアするための揮発性ランダムアクセスメモリ(RAM)を有し、このメモリは所定のパワー信号で動かされ、この結果、メモリの検査を可能にする第2の導電層の除去はパワーがメモリーから除去される。メモリが揮発性のために、これからパワーを除去するのはメモリにストアされている被保護データを消去することになる。

前記一実施例において、前記複数の揮発性メモリが夫々個別に、夫々のメモリと第2導電層の重なった場所のみから所定のパワー信号を受けられるように第2導電層のその場所のみと接続され、この結果、メモリを検査するためためにメモリを覆

っている第2の導電層の部分のみの除去は、この除去により露出したメモリからパワーが除去されるので、不都合である。

この発明に係わる集積回路チップにおいては、さらに非被保護データと制御信号が処理並びに／又はストアされ、前記のシールドされた回路要素は被保護領域と非被保護領域間の非被保護データ並びに／又は制御信号のトランスファーを可能にする第2の導電層により与えられる所定のパワー信号で動作するロジック回路要素を含むような非被保護領域をさらに具備する。この結果、被保護データがチップの非被保護領域に被保護領域から伝達されるのを可能にするブロープのような手段により、制御信号がロジック回路要素に送られるのを可能にするための第2の導電層の除去は、このような第2の導電層の除去がまたロジック回路要素からパワーを除去するので、好ましくない。このような実施例において、前記のロジック回路要素が夫々個別に第2導電層の重なった場所からのみ所定のパワー信号を受けるようにロジック回

路要素と重なった第2導電層のその場所に別々に接続されている。

この発明の別の態様において、前記の第1導電層のシールドされた回路要素は被保護データをストアするためのメモリと、そのメモリにストアされる駆動データ用のロジック回路を有し、その第2導電層はロジック回路の駆動機能にとって必須である信号を導き、しかもこの第2導電層の除去はこのメモリにデータがストアされることを妨げる。この結果、秘密データがチップの意図とした保護を損なう被保護データにメモリで代わられるのを可能とするロジック回路に制御信号を送るための第2の導電層の除去は、この第2の導電層の除去がロジック回路によってメモリにストフされるデータとなることを妨げるので好ましくない。

【実施例】

第1図に於て、本発明の集積回路チップ10の好ましい実施例は被保護領域11と非被保護領域12とを備えている。チップ10はVLSI (Very Large Scale Integrated) 回路チップであ

る。このチップ10は被保護領域11内に次の回路要素を形成している。即ち、被保護データを処理するマイクロプロセッサ14と、被保護データをストアする複数のメモリ M_1 、 M_2 、 M_n と、被保護データバス16と、被保護アドレスバス17と、移転ロジック回路18と、被保護クロック並びにパワー制御回路20とである。このチップ10はこのような回路要素の特別な混ぜ合せである必要はなく、その中で被保護データが無承諾の読み取り或は被保護データ並びに／又は指令の変更に対し保護されているような回路要素の或る組合せであってもよい。このメモリ M_1 、 M_2 、 M_n はどんなタイプでもよく、例えばRAM (ランダムアクセスメモリ)、ROM (読み取り専用メモリ)、EPROM (電氣的書込可能な読み取り専用メモリ)、EEPROM (電氣的消去書込可能な読み取り専用メモリ)等や、レジスタファイルやFIFO (ファストイン／ファストアウト)バッファ等である。

導電層 CN_2 は回路要素14、 M_1 、 M_2 、

M_n 、16、17、18、20を検査からシールドするためにこれらを覆っておりこうして被保護領域11を形成している。

非被保護領域12の中で、チップ10は次の如き回路要素を形成している。即ち、メモリ24とロジック回路26と非被保護データバス28とを形成している。

MOS回路要素を含むチップ10の実施例では第2図と第3図とに示す如く、このチップは半導体基板層SCと第1絶縁層 DE_1 と、第1導電層 CN_1 と、第2絶縁層 DE_2 と、第2導電層 CN_2 と、第n番目の絶縁層 DE_n と、n番目の導電層 CN_n とを有する。半導体基板層SCの中の拡散部分SとDは、ソースとドレンを形成し、それ等はゲート導体Gと組合され第1導電層 CN_1 により相互で接続されることでチップ10の回路要素を形成するために勢揃いしている相補性MOS電界効果トランジスタを形成している。第1導電層 CN_1 は第1絶縁層 DE_1 の孔を通し、導体30によりソースSとドレンDと接続されて

いる。第2導電層 CN_2 は第2絶縁層 DE_2 にある孔を通し、導体31により、シールドされた回路要素の予期機能に必須である所定の信号を回路要素に伝えるため第1導電層と接続されている。

第2導電層 CN_2 を除去することはこの回路要素に所定の必須の信号を伝えることを妨げ、従って予期機能もはばむことになるであろう。第2導電層 CN_2 は回路要素を覆い、その中で回路要素が検査からシールドされた被保護領域11を形成している。

バイポーラ回路要素を有するチップ10の実施例では、第4図に示す如く、このチップは半導体基板層 SC と、第1絶縁層 DE_1 と、第1導電層 CN_1 と、第2絶縁層 DE_2 と、第2導電層 CN_2 と、第 n 番目の絶縁層 DE_n と、 n 番目の導電層 CN_n とを有している。半導体層 SC 内の拡散部 C と B と E は、コレクタと、ベースと、エミッタとを形成し、これらはチップ10の回路要素を形成勢揃いしているバイポーラトランジスタを形成するために第1導電層 CN_1 により相互接

続されている。第1導電層 CN_1 は第1絶縁層 DE_1 にある孔を通し、導体32によりシールドされた回路要素の予期機能に必須である所定の信号を回路要素に伝えるためコレクタ C と、ベースとに接続されている。第2導電層 CN_2 は第2絶縁層 DE_2 にある孔を通じ導体33によりシールドされた回路要素の予期機能に必須である所定の信号を回路要素に伝えるため第1導電層 CN_1 と接続されている。

第2導電層 CN_2 の除去は、この回路要素に所定の必須の信号を伝えることを妨げ従って予期機能もはばむことになるであろう。第2導電層 CN_2 は回路要素を覆い、その中で回路要素が検査からシールドされた被保護領域11を形成している。

被保護データを配分し、ストアし処理し或は影響を与えるチップ10のすべての回路要素は、相互接続層 CN_1 の如き、あらかじめ作り込まれ、層 CN_2 の如く、シールドの特性を持ち、被保護領域11の境界を形成している導電層の下に位置

する導電層を利用している。

第2導電層 CN_2 は機械的とSEM(走査型電子顕微鏡)のプロビングに対するシールドとしての機能と、その下にある回路要素を動作不能にすることなしに除去出来ぬ所定の必須信号を伝達する層としての機能とを有する。所定の必須信号はパワー信号でも命令の如き制御信号でもよい。所定の必須信号がパワー信号である場合検査の目的でのシールド層 CN_2 の除去は機械的であれ化学的であれ或はその他の手段であれ下にある回路要素からパワーを除くこととなり動作不能にし更に多分同じ回路要素にストアされている何かのデータやロジックステートを失わせることになるだろう。

この技術は、特に揮発性RAMの如き揮発性メモリにストアされている被保護データを守るのに有効である。その中のメモリ M_1 と M_2 とが揮発性メモリであるチップ10の実施例に於て、このメモリ M_1 と M_2 は夫々検査からシールドするため第2導電層 CN_2 により覆われている。そして、

パワー信号は別々に夫々のメモリ M_1 、 M_2 と重っている第2導電層 CN_2 のポジションから夫々のメモリ M_1 、 M_2 に分配される。この分配は第5図に示され、第2導電層 CN_2 は揮発性メモリの中のトランジスタのソース S に導体34によりメモリパワーを配分するため接続されている。夫々のメモリ M_1 、 M_2 を検査するため第2導電層 CN_2 の重ったポジションを除去することは、夫々のメモリ M_1 、 M_2 からパワーを除くこととなる。メモリ M_1 、 M_2 は揮発性であるからそこからパワーを除くことはその中にストアされた被保護データを削除することとなる。従ってメモリ M_1 、 M_2 の内容をそのメモリに重っている第2導電層 CN_2 のポジションのみを除くことで検査しようと試みても無駄であろう。

第6図に示した他の実施例に於て、パワー信号 V_{cc} は第2導電層 CN_2 から複数の揮発性メモリ要素 M に前述の実施例よりも少ない大きさですむ方法、その中ではパワーは夫々のメモリ要素と重った第2導電層のポジションのみからメモリ要素

に別々に配分されるような方法で配られる。この実施例では夫々のメモリ要素Mの列は下にある別々の第1導電層CN₁を経由して重った第2導電層CN₂からパワーを受けとる。この第2導電層CN₂は夫々の第1導電層CN₁に導体35により接続されている。この実施例が面積効率を上げるため多少の安全を失ってもこれ等のメモリ要素Mを、第2導電層CN₂の除去によるパワー損失によるデータの消去を起すことなしに検査しようとすることはすべての中間層接続導体35とそれにパワーを供給する第2導電層CN₂のポーシオンに触れずにすると同時に非常に高い分解精度のある第2導電層の除去が求められるであろう。

今一度第1図に於て、非被保護領域12の中ではロジック要素26とメモリ24とは非保護データと制御信号を処理しストアする。非保護データと制御信号は非被保護データバス28から被保護領域11にある被保護データバス16に移転ロジック回路18により転送される。移転ロジック回路18は非被保護データと制御信号を被保護領域

11にある被保護データバス16にマイクロプロセッサ14により被保護データと処理するために転送する。転送ロジック回路18は非被保護データが被保護データバス16にある時に示すマイクロプロセッサ14により起される制御信号に呼応して非被保護データと制御信号が非保護データバス28と被保護データバス16の間に移転出来るようにする。マイクロプロセッサ14は被保護データバス16にあるデータ信号をモニターしロジック回路18が、データ信号と制御信号を非被保護データバス28と被保護データバス16の間に、非被保護データが被保護データバス16上にある間のみ転送可能とする制御信号を発生する。

上述の如く、導電層CN₂は移転ロジック回路18を検査からシールドする為に移転ロジック回路18に重っている。この導電層CN₂は又パワー信号を移転ロジック回路18に伝える。従って、移転ロジック回路18を検査する目的で導電層CN₂を除去することは移転ロジック回路18からパワーを除くことになり移転ロジック回路18

が何かのデータ或は制御信号を被保護データバス16と非被保護データバス28の間に移転することを妨げる。

この技術は逆方向にも拡張出来る。従って秘密のデータは非被保護領域12から被保護メモリM₁、M₂、M₃に書き込まれることはない。マイクロプロセッサ14は被保護データバス16にあるデータをメモリM₁、M₂、M₃にストア出来るようにするメモリアクセスロジック回路を備えており、シールドしている導電層CN₂はパワー信号をマイクロプロセッサ14に伝える。従って、制御信号をマイクロプロセッサ14のメモリアクセスロジック回路に伝えるため、従ってこのことはメモリM₁、M₂、M₃の中に内密のデータを被保護データの代りにすることが出来、従ってチップの予期された安全を危くすることとなるが、このためにシールドしている導電層CN₂を除去することは、この除去がマイクロプロセッサ14からパワーを除き従ってメモリアクセスロジック回路がメモリM₁、M₂、M₃にデータをス

トアさせることをさまたげるから無意味である。

1つの実施例に於ては被保護領域内のシールドされたロジック回路14、18は夫々別々にシールドしている導電層CN₂の重っているポーシオンのみからパワー信号を受けとるためにそのロジック回路14、18に重っているシールドしている導電層CN₂の夫々のポーシオンのみに接続されている。

第7図に示す実施例に於て、被保護信号はシールド層CN₂とCN₃の下にある導電層CN₁に配分される。そしてシールド信号(必須の制御或はパワー信号)は上に覆っているシールド層CN₂とCN₃に別々に配分される。1つのシールドしている導電層CN₁の境界は図中では実線で示され、他のシールドしている導電層CN₂の境界は図中に破線で示され、下にある導電層CN₁は図中ボカしで示される。下にある導電層CN₁は完全に1つか或は他のシールドしている導電層CN₂とCN₃によりシールドされている。そして下にある導電層CN₁の1つのポーシオン

はシールドしている導電層 CN_2 と CN_1 の両者によりシールドされている。

このシールド層 CN_2 と CN_1 を化学的或は普通のレーザ或はマイクロプローブで導電層 CN_1 中の被保護信号にアクセスするために切断すると言ふ試みは導電層 CN_1 に於てシールド層 CN_2 と CN_1 へ接続(短絡)されるか導電層 CN_1 と CN_2 と CN_1 で形成される回路でオープン回路が出来ることとなる。従つて、被保護信号と必須の信号の配分をばらばらにさせ導電層 CN_1 と CN_2 と CN_1 に接続されている回路要素の所期機能をチップ10の所期機能を害するように変化させる。

チップ10にストアされたある被保護データがそのチップの入った製品の製造中にその被保護データがストアされたあとは変更されないと云ふことは極めて重要である。この目的を成就するため、チップ10は所定のメモリロケーションにストアされた被保護データの変更を妨げるためのシステムを有している。このような予防システムの他の

フューズ要素はチップ10の中で金属性導電層とポリシリコンの導電層の組合せで形成される。アンチフューズ要素はチップの中で金属性導電層或はポリシリコンの導電層或は両者の組合せで形成される。アンチフューズ要素はチップの半導体層の中は導体/酸化物導体構造或は導体/アモルファスシリコン/導体構造により形成される P^+ / N^+ 半導体接合のダイオードと P^-/N^- 半導体接合のダイオードとにより作られる。

フューズ変更素子44は被保護領域11より外にあるターミナル50からライン48に来る所定の制御信号に呼応してフューズ要素42の状態を非可逆的に変化させるためにフューズ要素42と接続されている。更にライン48の制御信号は被保護領域11の内部にあるターミナル(図示していない)から供給される。

デテクター40はフューズ要素42の状態とアドレスバス46のアドレス信号をモニターするためメモリ制御回路38が所定のメモリロケーションが、アドレス信号によりアドレスバス46上

実施例を第8図と第9図とに示す。

第8図のシステムはメモリMと、メモリ制御ロジック回路38と、デテクター40と、フューズ要素42と、フューズ変更素子44を有する。このシステムはメモリMに適用されその中に被保護データがストアされる夫々のメモリ M_1 、 M_2 、 M_3 がメモリMとして含まれている。

このメモリMはデータバス16からの変更不能なデータをストアする所定のロケーションである複数のメモリロケーションを持っている。

メモリ制御ロジック回路38はアドレスバス46により“書き込み”信号がライン47上でメモリ制御ロジック回路38から被保護メモリMに与えられた場合ユーザデータがアドレスバス46に与えられたアドレス信号により指示されたメモリMのロケーションにストアされるためにメモリMに接続されている。

フューズ要素42は最初の状態と非可逆的に変化した状態を持っている。“フューズ要素”と云う言葉はフューズとアンチフューズを云っている。

に示される時は何時でもフューズ要素の状態が非可逆的に変更してしまったあとでメモリMの所定のメモリロケーションにコーディングデータがストアされるのを防ぐためにフューズ要素42とメモリ制御回路38とアドレスバス46とに接続されている。

第2導電層 CN_2 は、メモリMとメモリ制御ロジック回路38とデテクター40とフューズ要素42とを外部からの直接アクセスからシールドしている。

メモリMとメモリ制御ロジック回路38とデテクター40は第2導電層 CN_2 から来るパワー信号によって動かされるようにすべて第2導電層 CN_2 に接続されている。

第8図のシステムはメモリMの所定のロケーションに最初からストアされた被保護データの変更を防ぐのに使われる。フューズ要素42の状態が非可逆的に変化した場合、デテクター40はアドレスバス46のアドレス信号により示された所定のメモリロケーションに何らかの追加データが書

込まれるのを防ぐ。

第8図のシステム中のフューズ要素42は又このチップを使っている製品がその使用者にとどく時に先だつてのみ適用出来るある予備的な被保護データ処理機能、例えば被保護データの予備的処理或は被保護データを処理するインストラクションのローディングを行ったりそれに影響したりする他のシールドされた回路要素(図に示されていない)に接続されることもある。デテクター40の如きものはフューズ要素をモニターするため、フューズ要素の状態が非可逆的に変化したあとでは他のシールドされた回路要素の予期された機能を妨げるためにフューズ要素42と他のシールドされた回路要素に接続されている。

多くのフューズ技術は、被保護集積回路チップの製造工程中工場でのみフューズすることを可能にする。例えば、ある工場は素子のよりよい長期信頼性を得るためにフューズが溶けたあと、ポリシリコン(或は他のフューズ材料)上に酸化物を成長させることを要求している。第9図にシステ

ションを持っている。

駆動回路55は、書込駆動信号がライン63を通じ駆動回路55に加えられたとき、消去可能メモリ52にデータパターンをストアされるようにする。

メモリ制御ロジック回路54は消去可能なメモリ52が所定のデータパターンを入れている時は何時でもライン64からANDゲート60への書込み信号に呼応して第1メモリMの所定のロケーションにデータがストアされるようにメモリMと消去可能なメモリ52と接続されている。

消去可能なメモリ52の内容はチップ10の被保護領域11の外部にある消去ターミナル66から“消去”の制御信号が与えられることで消され得る。

フューズ要素56は、最初の状態と非可逆的に変化した状態とを持っている。フューズ変更素子58は被保護領域11の外部にあるターミナル68からライン67に与えられる所定の制御信号に呼応してフューズ要素56の状態を非可逆的に

ムは、別の製造者が工場でのフューズの後、被保護メモリMへ被保護データを入力することを可能にしているが、被保護メモリMの内容の変更を妨げている。

第9図のシステムはメモリMと、EPROM或はEEPROM(電氣的消去可能なROM)の如き消去可能なメモリ52と、メモリ制御ロジック回路54と、エネープリング回路(駆動回路)55と、フューズ要素56と、ANDゲート57と、フューズ変更素子58とを有する。メモリ制御ロジック回路54はANDゲート60と、ANDゲート60と消去可能なメモリ52とを結ぶインバータ62、並びに配線を含むN接続とを備えている。インバータ62はANDゲート60への選ばれた入力とANDゲート60を働かせるには必要な消去可能メモリ52中に所定のデータパターンを形成する如き消去可能なメモリ52中の選ばれたメモリロケーションとの間に接続されている。

メモリMは変更不能な被保護データをストアする所定のロケーションである複数のメモリロケー

ションを持つ。更にライン67の制御信号は被保護領域11の内部にあるターミナル(図示していない)から供給される。

データパターンはデータターミナル69から供給されANDゲート57を通じ消去可能なメモリに供給される。ANDゲート57はフューズ要素56が最初の状態にある間のみ消去可能メモリ52にデータを書込ませることが出来るようにフューズ要素56につながる1つの入力をもっている。

フューズ要素56は又フューズ要素56の状態が非可逆的に変化変化する前のみ消去可能なメモリ52に所定のデータパターンをストアさせられるように駆動回路55と接続されている。

消去可能なメモリ52はNビットが必要である。工場では、消去可能なメモリ52とANDゲート60とに接続されたインバータ62に対応して所定の1, 0のパターンがANDゲート60がライン64を通じメモリMに“書込み”制御信号がバ

ス出来るように消去可能なメモリ52に入れられる。1, 0の所定のパターンが消去可能なメモリ52に入れられたあと、フューズ要素56の状態が非可逆的に変化されると所定のパターンは変更出来ない。この点で集積回路チップ10の処理やパッケージングは接続可能となり消去可能なメモリ52にストアされた所定のパターンを乱すことなく最終処理とパッケージングが出来るようになる。

チップ10が別の製造者に出荷されたあと被保護データは被保護メモリMにストアされる。それは消去可能なメモリ52にストアされた所定のパターンは、インバータ62によりメモリ制御ロジック回路54に入れられた所定のパターンに匹適しているからである。

被保護データが被保護メモリMにストアされると“消去”信号が消去可能なメモリ52の内容を消去するために消去ターミナル66に加えられても被保護メモリMの中の被保護データは変化しない。第2導電層CN₂はメモリMと、消去可能な

メモリ52と、メモリ制御ロジック回路54と、駆動回路55と、フューズ要素56とを直接的な外部からのアクセスからシールドしている。

この技術は第9図のシステムをチップ10のカバー層を通し消去可能なメモリ52を遠くからプログラム仕直せるような非常に正確なX線ビームのショットや他の複雑な手段から守ることが出来る。この技術の安全はEEROMやFPRMの内容を遠くからプログラムし直すこと或はとけたフューズを再接続することは非常に困難だと云うことに由っている。若し非常に強力な焦点の定まらない或は発散性X線或は他の手段が、EEROM或はEPRMの内容を本質的に無作為化することが出来るとすれば、攻撃者は駆動パターンを完成させる企をくりかえすこととなる。従って安全はEEROM或はEPRMセルがこれ等の状態によって偏って設けられる。

第9図に示すシステムのフューズ要素56は、所定の被保護データプロセス機能を果たすように、他のシールド回路要素(図示せず)に接続さ

れ得る。この機能は、被保護データの前処理や被保護データの処理のための検査のように、チップを含む製品が製品の使用者に渡る前にのみ適用できる。フューズ要素56は、フューズ要素56の状態が非可逆的に変更される前にのみ、他のシールド回路要素の意図した機能が果たせるように、他のシールド回路要素に接続される。

第8図並びに第9図に示す被保護データ変更防止システムは“Prevention of Alternation of Data Stored in Secure Integrated Circuit Chip Memory”と題する同じ出願人による先願の主題である。

複雑な集積回路の製造は、全ての回路素子が正確に動作するようにするテスト操作の間、内部回路素子への完全なアクセスを必要とする。しかし、テストのための高いアクセス可能性は、被保護データもしくは変更されないデータを含むチップに対しては問題である。

第10図は、テスト動作が完了した後に、テスト信号バスを永久的に無能にし、この結果チッ

プの外部ピンからの内部被保護データ回路要素へアクセスをさらにする必要を無くすシステムを示す。このシステムはフューズ要素70と、第1並びに第2のインバータ72, 74と、抵抗75と、第1並びに第2のNANDゲート76, 78と、フューズ変更装置79とを有する。

前記フューズ要素70は最初の状態と、非可逆で変化した状態とを呈する。フューズ変更装置79はフューズ要素70に接続され、被保護領域11の外部のターミナル81からライン80により受信する所定の制御信号に応答して、フューズ要素70の状態を非可逆的に変化させる。代わって、ライン80への制御信号は被保護領域11の内部のターミナル(図示せず)から受信する。

前記フューズ要素70とインバータ72, 74とは第1のNANDゲート76への1つの入力に直列に接続されている。このNANDゲート76の出力信号は外部テストデータ出力ターミナルに与えられる。

前記フューズ要素70とインバータ72、74とは、また第2のNANDゲートの出力ターミナル82の1つの入力に直列に接続されている。

前記第2のNANDゲート78は、チップ10の被保護領域11内のテストコマンド入力ノード86への外部テストコマンド入力ターミナル84からのテストコマンド信号を通す。テストコマンド入力信号がテストコマンド入力ノード86に与えられるのに応答して、テストデータがチップ10の被保護領域11内のテストコマンド出力ノード88に与えられる。内部テストデータ出力ターミナルに与えられるテストデータは、回路要素14、 M_1 、 M_2 、 M_3 、16、17、18、20(第1図に示す)のようなチップ10の被保護データ要素からアクセスされ得る。

前記テストデータは、フューズ要素70が最初の状態のときにのみ、テストコマンド出力ノード88から、第1のNANDゲート76を介して、外部テストデータ出力ターミナル82に与えられる。

また、テストコマンド入力信号は、フューズ要素が最初の状態のときにのみ、外部テストコマンド入力ターミナル84から内部テストコマンド入力ノード86に与えられる。

前記第2の導電層 CN_2 は、直接的な外部アクセスから、フューズ要素70と、インバータ72、74と、抵抗75と、NANDゲート76、78とをシールドする。

前記インバータ72、74と、抵抗75と、NANDゲート76、78とは、全て第2の導電層 CN_2 に接続され、第2の導電層 CN_2 からのパワー信号により駆動される。

プローブによる被害を防止するように、可能な限りチップ10内に深く、フューズ要素70から第1並びに第2のNANDゲート76、78への信号バスを埋め込むことにより、付加的保護がなされる。かくして、フューズ要素70から第1並びに第2のNANDゲート76、78への信号バスは、主として、 N^+ 、 P^+ 拡散により形成される。同様に最小の保護で、ポリシリコン並びに

他の導電層が使用され得る。最上の導電層 CN_n 、 CN_{n-1} の使用は避けることが好ましい。

4. 図面の簡単な説明

第1図は本発明による集積回路チップのブロックダイヤグラムである。

第2図は本発明による集積回路チップにおけるMOS回路要素を示す断面図である。

第3図は回路要素をシールドしシールドされたMOS回路要素へ所定の信号を送る重った導電層を示す平面図である。

第4図は本発明の集積回路チップにおけるバイポーラ回路要素のシールドングを示す断面図である。

第5図は回路要素をシールドしシールドされた回路要素に電力を供給するための重った導電層を示す断面図である。

第6図は複数の揮発性メモリをシールドしている別の実施例のブロックダイヤグラムである。

第7図は回路要素の機能へ必須信号を送る重った導電層を示す平面図である。

第8図は被保護領域内で所定のロケーションにストアされた被保護データを変更することを妨げるシステムの実施例のブロックダイヤグラムである。

第9図は被保護領域内で所定のメモリロケーションにストアされた被保護データの変更を防ぐシステムの別の実施例のブロックダイヤグラムを示す。

第10図は被保護領域がテストのためにアクセスされた時に制限を加えるチップ内被保護領域でのシステムの適当な実施例のブロックダイヤグラムである。

10…チップ、11…被保護領域、14…マイクロプロセッサ、 M_1 、 M_2 、 M_3 …メモリ、16…被保護データバス、17…被保護アドレスバス、18…移転ロジック回路、20…パワー制御回路、SC…半導体基板層、 DE_1 …第1絶縁層、 CN_1 …第1導電層、 DE_2 …第2絶縁層、 CN_2 …第2導電層、S、D…拡散部分。

出願人代理人 弁理士 鈴江武彦

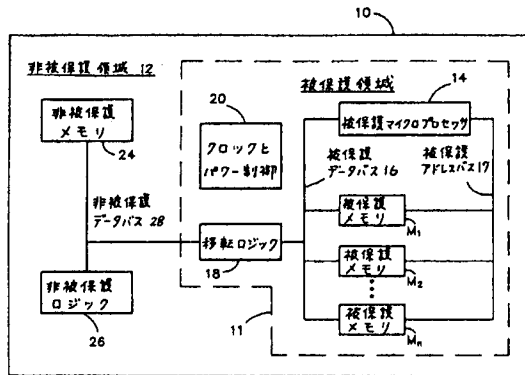


FIG. 1

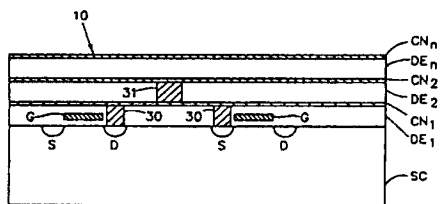


FIG. 2

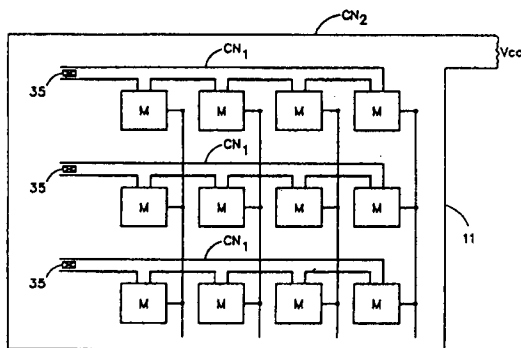


FIG. 6

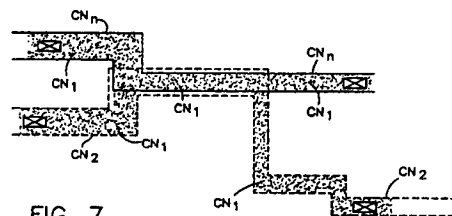


FIG. 7

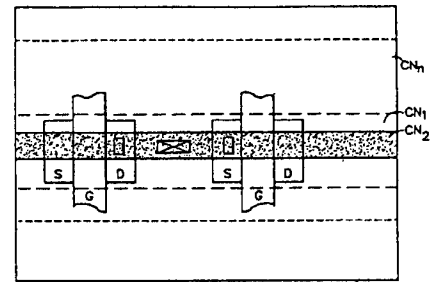


FIG. 3

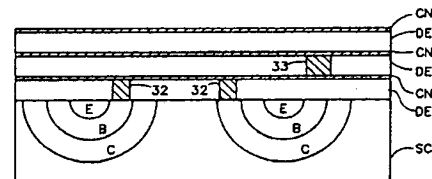


FIG. 4

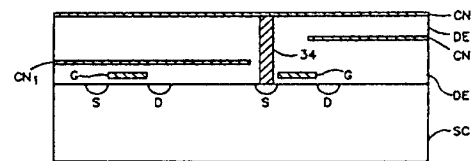


FIG. 5

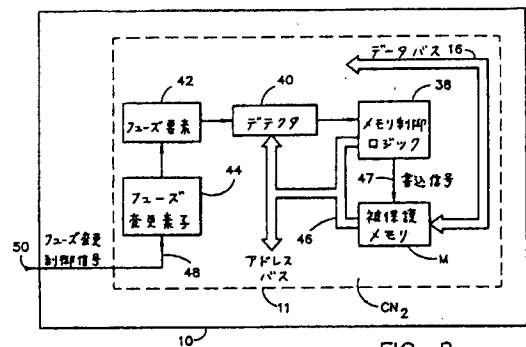


FIG. 8

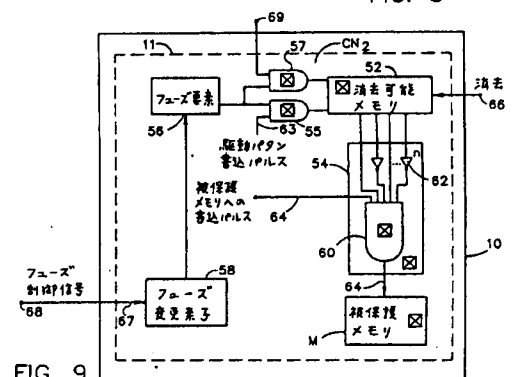


FIG. 9

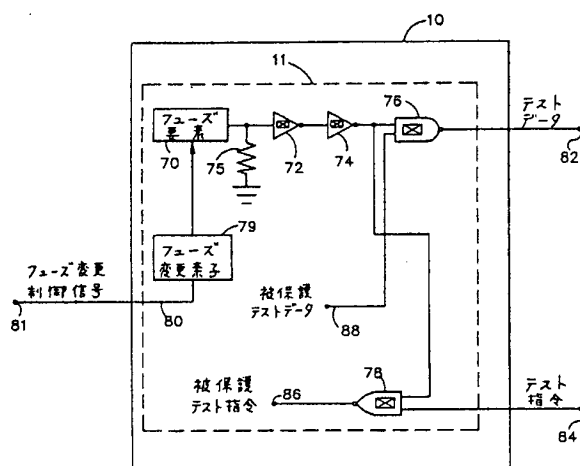


FIG. 10

第 1 頁の続き

⑤Int. Cl. ³

識別記号

庁内整理番号

H 01 L 21/82
29/788
29/792

⑦②発 明 者 ボール・マロニー

アメリカ合衆国、カリフォルニア州 92007、カーディフ
 バイヤー・ザ・シー、アボセット・コート 1249

⑫発 明 者 ウイリアム・アレン・
 シュメイト

アメリカ合衆国、カリフォルニア州 92116、サンディエ
ゴ、ビオナ・プレイス 4202